

93^d CONGRESS
1ST SESSION

H. R. 10042

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 5, 1973

MR. GOLDWATER introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To provide standards of fair personal information practices.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 SECTION 1. This Act may be cited as the "Code of Fair
4 Information Practices of 1973".

5 FINDINGS AND DECLARATION OF PURPOSE

6 SEC. 2. (a) The Congress finds—

7 (1) that an individual's personal privacy is directly
8 affected by the kind of disclosure and use made of iden-
9 tifiable information about him in a record;

10 (2) that a record containing information about an
11 individual in identifiable form must be governed by

I

1 procedures that afford the individual a right to partici-
2 pate in deciding what the content of the record will be,
3 and what disclosure and use will be made of the identi-
4 fiable information in it;

5 (3) that any recording, disclosure, and use of iden-
6 tifiable personal information by an organization not
7 governed by such procedures must be proscribed as an
8 unfair information practice unless such recording, dis-
9 closure, or use is specifically authorized by Federal
10 statute.

11 (b) The purpose of this Act is to insure safeguards for
12 personal privacy from recordkeeping organizations by ad-
13 herence to the following principles of information practice:

14 (1) There must be no personal data recordkeeping
15 systems whose very existence is secret.

16 (2) There must be a way for an individual to find
17 out what information about him is in a record and how it
18 is used.

19 (3) There must be a way for an individual to pre-
20 vent information about him obtained for one purpose
21 from being used or made available for other purposes
22 without his consent.

23 (4) There must be a way for an individual to cor-
24 rect or amend a record of identifiable information about
25 him.

1 things done by or to an individual such as records of financial
2 transactions, medical treatment, or other services; or that
3 afford a clear basis for inferring personal characteristics or
4 things done by or to an individual, such as the mere record
5 of his presence in a place, attendance at a meeting, or ad-
6 mission to some type of service institution.

7 (d) The term "computer accessible" means recorded on
8 magnetic tape, magnetic disk, magnetic drum, punched card,
9 or optically scannable paper or film.

10 (e) The term "data system" includes all processing op-
11 erations, from initial collection of data through all uses of
12 the data, including outputs from the system. Data recorded on
13 questionnaires, or stored in microfilm archives, are consid-
14 ered part of a data system, even when the computer-accessi-
15 ble files themselves do not contain identifying information.

16 (f) The term "organization" means any Federal agen-
17 cy; the courts of the United States; the government of the
18 District of Columbia; any public or private corporation, part-
19 nership, agency, or association which operates an adminis-
20 trative automated personal data system, or a statistical-
21 reporting and research automated personal data system; and
22 which is supported in whole or in part by Federal funds,
23 Federal systems, or federally supported systems, or which
24 directly or indirectly makes use of any means or instruments
25 of transportation or communications in interstate commerce,

1 or of the mails, or which carries or causes to be carried in the
2 mails or interstate commerce, or by any other means or in-
3 struments of transportation any personal data; and any orga-
4 nization which maintains a record of individually identifiable
5 personal data which it does not maintain as part of an admin-
6 istrative or as a statistical-reporting and research automated
7 personal data system and which transfers such data to one of
8 the above organizations in interstate commerce.

9 (g) The term "administrative personal data system"
10 means one that maintains data on individuals for the purpose
11 of affecting them directly as individuals; and for making
12 determinations relating to their qualifications, character,
13 rights, opportunities, or benefits.

14 (h) The term "statistical-reporting or research system"
15 means one that maintains data about individuals exclusively
16 for statistical reporting or research and is not intended to be
17 used to affect any individual directly.

18 (i) The term "unfair personal information practice"
19 means a failure to comply with any safeguard requirements
20 of this Act.

21 (j) The term "data subject" means the individual whose
22 name or identity is added to or maintained on an automated
23 personal data system or a statistical-reporting or research
24 system.

1 SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE
2 PERSONAL DATA SYSTEMS

3 SEC. 4. (a) GENERAL REQUIREMENTS.—(1) Any or-
4 ganization maintaining a record of individually identifiable
5 personal data, which it does not maintain as part of an ad-
6 ministrative automated personal data system, shall make no
7 transfer of any such data to another organization, without
8 the prior informed consent of the individual to whom the
9 data pertain, if, as a consequence of the transfer, such data
10 will become part of an administrative automated personal
11 data system that is not subject to these safeguard require-
12 ments.

13 (2) Any organization maintaining an administrative
14 automated personal data system shall—

15 (A) identify one person immediately responsible for
16 the system, and make any other organizational arrange-
17 ments that are necessary to assure continuing attention
18 to the fulfillment of these safeguard requirements;

19 (B) take affirmative action to inform each of its
20 employees having any responsibility or function in the
21 design, development, operation, or maintenance of the
22 system, or the use of any data contained therein, about
23 all these safeguard requirements and all the rules and
24 procedures of the organization designed to assure com-

1 pliance with them, and the nature of such action shall
2 be supplied upon the reasonable request of a data subject;

3 (C) specify penalties to be applied to any employee
4 who initiates or otherwise contributes to any disciplinary
5 or other punitive action against any individual who brings
6 to the attention of appropriate authorities, the press, or
7 any member of the public, evidence of unfair personal
8 information practice;

9 (D) take reasonable precautions to protect data in
10 the system from any anticipated threats or hazards to
11 the security of the system;

12 (E) make no transfer of individually identifiable
13 personal data to another system without (i) specifying
14 requirements for security of the data, including limita-
15 tions on access thereto, and (ii) determining that the
16 conditions of the transfer provide substantial assurance
17 that those requirements and limitations will be ob-
18 served—except in instances when an individual specifi-
19 cally requests that data about him be transferred to an-
20 other system or organization;

21 (F) maintain a complete and accurate record of
22 every access to and use made of any data in the system,
23 including the identity of all persons and organizations to
24 which access has been given;

1 (G) maintain data in the system with which such
2 accuracy, completeness, timeliness, and pertinence as is
3 necessary to assure accuracy and fairness in any deter-
4 mination relating to an individual's qualifications, char-
5 acter, rights, opportunities, or benefits, that may be
6 made on the basis of such data.

7 (b) Any organization maintaining an administrative
8 automated personal data system that publicly disseminates
9 statistical reports or research findings based on personal data
10 drawn from the system, or from systems of other organiza-
11 tions, shall—

12 (1) make such data publicly available for inde-
13 pendent analysis, on reasonable terms; and

14 (2) take reasonable precautions to assure that no
15 data made available for independent analysis will be
16 used in a way that might reasonably be expected to
17 prejudice judgments about any individual data subject's
18 character, qualifications, rights, opportunities, or bene-
19 fits.

20 (c) PUBLIC NOTICE REQUIREMENT.—Any organization
21 maintaining an administrative automated personal data sys-
22 tem shall give public notice of the existence and character
23 of its system once each year, in the case of Federal organiza-
24 tions in the Federal Register, or in the case of other organiza-
25 tions, in a media likely to bring attention to the evidence of

1 the records to the data subject. Any organization maintain-
2 ing more than one system shall publish such annual notices
3 for all its systems simultaneously. Any organization propos-
4 ing to establish a new system, or to enlarge an existing sys-
5 tem, shall give public notice long enough in advance of the
6 initiation or enlargement of the system to assure individuals
7 who may be affected by its operation a reasonable opportu-
8 nity to comment. The public notice shall specify:

9 (1) The name of the system.

10 (2) The nature and purpose (s) of the system.

11 (3) The categories and number of persons on whom
12 data are (to be) maintained.

13 (4) The categories of data (to be) maintained, in-
14 dicating which categories are (to be) stored in computer-
15 accessible files.

16 (5) The organization's policies and practices re-
17 garding data storage, duration of retention of data, and
18 disposal thereof.

19 (6) The categories of data sources.

20 (7) A description of all types of use (to be) made
21 of data, indicating those involving computer-accessible
22 files, and including all classes of users and the organiza-
23 tional relationships among them.

24 (8) The procedures whereby an individual can (A)
25 be informed if he is the subject of data in the systems;

1 (B) gain access to such data; and (C) contest their
2 accuracy, completeness, timeliness, pertinence, and the
3 necessity for retaining it.

4 (9) The procedures whereby an individual, group,
5 or organization can gain access to data used for statisti-
6 cal reporting or research in order to subject such data
7 to independent analysis.

8 (10) The title, name, and address of the person
9 immediately responsible for the system.

10 (11) A description of the penalties to be applied
11 to any employee who initiates or otherwise contributes to
12 any disciplinary or other punitive action against any indi-
13 vidual who brings attention to any evidence of unfair
14 information practices.

15 (d) RIGHTS OF INDIVIDUAL DATA SUBJECTS.—Any
16 organization maintaining an administrative automated per-
17 sonal data system shall—

18 (1) inform an individual asked to supply personal
19 data for the system whether he is legally required, or
20 may refuse, to supply the data requested, and also of
21 any specific consequences for him, which are known to
22 the organization, of providing or not providing such
23 data;

24 (2) upon request and proper identification of any

11

1 data subject, clearly and accurately disclose to the data
2 subject, in a form comprehensible to him—

3 (A) all data about the data subject;

4 (B) the sources of the information;

5 (C) the recipients of any transfer, report, dis-
6 semination, or use of data about the data subject,
7 including the identity of all persons and organiza-
8 tions involved and their relationship to the system;

9 (3) comply with the following minimum conditions
10 of disclosure to data subjects—

11 (A) an organization shall make the disclosures
12 required under subsection 4 (d) (2) during normal
13 business hours;

14 (B) the disclosures required under section 4
15 (d) (2) shall be made to the data subject (i) in
16 person if he appears in person and furnishes proper
17 identification; the data subject is entitled to personal,
18 visual inspection of data about him; or (ii) by tele-
19 phone if he has made a written request, with proper
20 identification; telephone disclosures are to be made
21 without charge to the data subject; and (iii) by mail
22 if he has made a written request, with proper identi-
23 fication; and (iv) by providing a copy of his file, if

1 requested, at a charge not to exceed 10 cents per
2 page;

3 (C) the data subject shall be permitted to be
4 accompanied by one person of his choosing, who
5 shall furnish reasonable identification. An organiza-
6 tion may require the data subject to furnish a writ-
7 ten statement granting permission to the organiza-
8 tion to discuss the data subject's file in such per-
9 son's presence;

10 (D) subsection 4 (d) (2) disclosure, shall not
11 apply to subject files that are (i) directly related
12 to international relations or international subversive
13 activities, or (ii) active criminal investigatory data,
14 except active criminal investigatory data which has
15 been maintained for a period longer than reasonably
16 necessary to bring indictment, information, or to
17 commence prosecution.

18 (4) assure that no use of individually identifiable
19 data is made that is not within the stated purposes of
20 the system as reasonably understood by the individual,
21 unless, in the case of each use of such data, the informed
22 consent of the individual has been obtained in writing;

23 (5) assure that no data about an individual is made
24 available from the system in response to a demand for
25 data made by means of compulsory legal process, unless

1 the individual to whom the data pertain has been noti-
2 fied of the demand; and

3 (6) if the completeness, accuracy, pertinence, time-
4 liness, or necessity for retaining the data in the system is
5 disputed by the data subject and the dispute is directly
6 conveyed to the organization by the data subject, the
7 following minimum procedures shall be followed:

8 (A) The organization shall within a reasonable
9 period of time investigate and record the current
10 status of that data unless it has reasonable grounds
11 to believe that the dispute by the data subject is
12 frivolous or irrelevant.

13 (B) If, after such investigation, such data is
14 found to be inaccurate or can no longer be verified,
15 the organization shall promptly delete such data.

16 (C) The presence of contradictory informa-
17 tion in the data subject's file does not in and of
18 itself constitute reasonable grounds for believing the
19 dispute is frivolous or irrelevant.

20 (D) If the investigation does not resolve the
21 dispute, the data subject may file a brief statement
22 setting forth the nature of the dispute; the orga-
23 nization may limit such statements to not more than
24 one hundred words if the organization provides the

1 data subject with assistance in writing a clear sum-
2 mary of the dispute.

3 (E) Whenever a statement of a dispute is filed,
4 unless there are reasonable grounds to believe that
5 it is frivolous or irrelevant, the organization shall, in
6 any subsequent transfer, report, or dissemination of
7 the data in question, clearly note that it is disputed
8 by the data subject and provide either the data sub-
9 ject's statement or a clear and accurate summary
10 thereof.

11 (F) Following any deletion of data which is
12 found to be inaccurate or whose accuracy can no
13 longer be verified or any notation as to disputed
14 data, the organization shall, at the request of the
15 data subject, furnish notification that the item has
16 been deleted, or a statement, or summary, which
17 contains the deleted or disputed information to any
18 person specifically designated by the data subject.

19 (i) The organization shall clearly and
20 conspicuously disclose to the data subject his
21 rights to make such a request.

22 SAFEGUARD REQUIREMENTS FOR STATISTICAL-REPORTING
23 AND RESEARCH SYSTEMS

24 SEC. 5. (a) GENERAL REQUIREMENTS.—(1) Any or-
25 ganization maintaining a record of personal data, which it

1 system used exclusively for statistical-reporting or research,
2 shall make no transfer of any such data to another organiza-
3 tion without prior informed consent of the individual to whom
4 the data pertain, if, as a consequence of the transfer, such
5 data will become part of an automated personal data system
6 that is not subject to these safeguard requirements or the
7 safeguard requirements for administrative personal data
8 systems.

9 (2) Any organization maintaining an automated per-
10 sonal data system used exclusively for statistical-reporting
11 or research shall—

12 (A) identify one person immediately responsible
13 for the system, and make any other organizational ar-
14 rangements that are necessary to assure continuing at-
15 tention to the fulfillment of the safeguard requirements;

16 (B) take affirmative action to inform each of its
17 employees having any responsibility or function in the
18 design, development, operation, or maintenance of the
19 system, or the use of any data contained therein, about
20 all the safeguard requirements and all the rules and pro-
21 cedures of the organization designed to assure compliance
22 with them;

23 (C) specify penalties to be applied to any employee
24 who initiates or otherwise contributes to any disciplinary
25 or ~~other~~ punitive action against any individual who

1 brings to the attention of appropriate authorities, the
2 press, or any member of the public, evidence of unfair
3 personal information practice;

4 (D) take reasonable precautions to protect data
5 in the system from any anticipated threats or hazards
6 to the security of the system;

7 (E) make no transfer of individually identifiable
8 personal data to another system without (i) specifying
9 requirements for security of the data, including limita-
10 tions on access thereto, and (ii) determining that the
11 conditions of the transfer provide substantial assurance
12 that those requirements and limitations will be ob-
13 served—except in instances when each of the individu-
14 als about whom data is to be transferred has given his
15 prior informed consent to the transfer; and

16 (F) have the capacity to make fully documented
17 data readily available for independent analysis.

18 (b) PUBLIC NOTICE REQUIREMENT.—Any organiza-
19 tion maintaining an automated personal data system used
20 exclusively for statistical-reporting or research shall give
21 public notice of the existence and character of its system
22 once each year, in the case of Federal organizations in the
23 Federal Register, or in the case of other organizations, in
24 a media likely to bring attention to the existence of the rec-
25 ords to the data subject. Any organization maintaining more

1 than one such system shall publish annual notices for all its
2 systems simultaneously. Any organization proposing to es-
3 tablish a new system, or to enlarge an existing system, shall
4 give public notice long enough in advance of the initiation
5 or enlargement of the system to assure individuals who may
6 be affected by its operation a reasonable opportunity to
7 comment. The public notice shall specify—

8 (1) the name of the system;

9 (2) the nature and purpose (s) of the system;

10 (3) the categories and number of persons on whom
11 data are (to be) maintained;

12 (4) the categories of data (to be) maintained, indi-
13 cating which categories are (to be) stored in computer-
14 accessible files;

15 (5) the organization's policies and practices regard-
16 ing data storage, duration of retention of data, and dis-
17 posal thereof;

18 (6) the categories of data sources;

19 (7) a description of all types of use (to be) made
20 of data, indicating those involving computer-accessible
21 files, and including all classes of users and the organiza-
22 tional relationships among them;

23 (8) the procedures whereby an individual, group,
24 or organization can gain access to data for independent
25 analysis;

1 (9) the title, name, and address of the person im-
2 mediately responsible for the system;

3 (10) a statement of the system's provisions for data
4 confidentiality and the legal basis for them.

5 (c) RIGHTS OF INDIVIDUAL DATA SUBJECTS.—Any
6 organization maintaining an automated personal data system
7 used exclusively for statistical-reporting or research shall—

8 (1) inform an individual asked to supply personal
9 data for the system whether he is legally required, or
10 may refuse, to supply the data requested, and also of any
11 specific consequences for him, which are known to the
12 organization, of providing or not providing such data;

13 (2) assure that no use of individually identifiable
14 data is made that is not within the stated purposes of
15 the system as reasonably understood by the individual,
16 unless, in the case of each use of such data, the informed
17 consent of the individual has been explicitly obtained;

18 (3) assure that no data about an individual and
19 made available from the system in response to a demand
20 for data made by means of compulsory legal process,
21 unless the individual to whom the data pertain—

22 (A) has been notified of the demand, and

23 (B) has been afforded full access to the data
24 before they are made available in response to the
25 demand.

ENFORCEMENT

1
2 SEC. 6. (a) INJUNCTIONS FOR COMPLIANCE.—When-
3 ever it appears to the Attorney General of the United States
4 that any organization has engaged, is engaged, or is about
5 to engage in any acts or practices constituting an unfair per-
6 sonal information practice under this Code, he may by his
7 own discretion bring an action, in the district court of the
8 United States or the appropriate United States court of any
9 territory or other place subject to the jurisdiction of the
10 United States, to enjoin such acts or practices, and showing
11 there is or is about to be such engagement, a permanent or
12 temporary injunction or restraining order shall be granted
13 without bond. Upon application of the Attorney General
14 any such court may also issue injunctions commanding any
15 organization to comply with any section of the Code. The
16 court may grant as relief, as it deems appropriate, any per-
17 manent, or temporary injunction, temporary restraining order,
18 or other order, at the prayer of a data subject or class of data
19 subjects.

20 (b) CIVIL LIABILITY FOR UNFAIR PERSONAL INFOR-
21 MATION PRACTICE.—Any organization which commits an
22 unfair personal information practice shall be liable in an
23 amount equal to the sum of—

24 (1) any actual damages sustained by the data sub-

1 ject(s) as a result of the unfair practice, but not less
2 than liquidated damages of \$10,000; and

3 (2) such amount of punitive damages as the court
4 may allow; and

5 (3) in the case of any successful action to enforce
6 any liability under this section, the costs of the action
7 together with reasonable attorney's fees as determined
8 by the court.

9 (c) CRIMINAL LIABILITY FOR UNFAIR PERSONAL IN-
10 FORMATION PRACTICES BY FEDERAL OFFICERS OF EM-
11 PLOYEES.—Any officer or employee of any Federal agency,
12 the courts of the United States, the governments of the terri-
13 tories or possessions of the United States, or the government
14 of the District of Columbia who willingly or knowingly per-
15 mits or causes to occur an unfair personal information prac-
16 tice shall be fined not more than \$10,000 or imprisoned not
17 more than one year or, suspended from employment without
18 pay for not more than one year, or all three.

19 (d) JURISDICTION OF COURTS; LIMITATIONS OF AC-
20 TIONS.—An action to enforce any liability created under this
21 Code may be brought in any appropriate United States dis-
22 trict court without regard to the amount in controversy, or
23 in any other court or competent jurisdiction, within two
24 years from the date on which the liability arises, except
25 where a defendant has materially and willfully failed to com-

1 ply with the safeguards under this Code, the action may be
2 brought at any time within two years after discovery by the
3 individual data subject.

4 SEVERABILITY

5 SEC. 7. If any provision of this Code or the appli-
6 cation thereof to any particular circumstance or situation is
7 held invalid, the remainder of this Code, or the application
8 of such provision to any other circumstance or situation shall
9 not be affected thereby.

10 EFFECTIVE DATE

11 SEC. 8. This Code shall take effect one year after
12 the date of its enactment.

13 STATE LAWS

14 SEC. 9. (a) No State law in effect on the date of
15 passage of this Act or which may become effective there-
16 after shall be superseded by any provision of this Code except
17 insofar as such State law is in conflict with this Code.

18 (b) The provisions of any State law or regulation in
19 effect upon the effective date of this Act, or which may be-
20 come effective thereafter, which provide for more stringent
21 safeguard standards than do the provisions of this Code shall
22 not thereby be construed or held to be in conflict with this
23 Code. The provisions of any State law or regulation in effect
24 upon the operative date of this Act, or which become effec-
25 tive thereafter, which provide for safeguard standards for

1 which no provision is contained in this Code shall not be
2 held to be in conflict with this Code.

3 FEDERAL AGENCY REGULATIONS

4 SEC. 10. (a) Each Federal agency shall, with the
5 advice of the Attorney General of the United States pursuant
6 to the Administrative Procedure Act, promulgate, adopt, and
7 from time to time amend and administer comprehensive rules
8 and regulations necessary to further the purposes of this Act
9 for the internal activities of such agency and in a manner
10 consistent with the safeguards specified herein.

11 (b) Notwithstanding any statute or regulation to the
12 contrary, rules and regulations issued hereunder shall govern
13 and control the collection, security, and dissemination of all
14 automated personal data by each Federal agency.

Approved For Release 2002/05/01 : CIA-RDP82-00357R000700120015-0

93d CONGRESS
1st Session

H. R. 10042

A BILL

To provide standards of fair personal information practices.

By Mr. GOLDWATER

SEPTEMBER 5, 1973

Referred to the Committee on the Judiciary

Approved For Release 2002/05/01 : CIA-RDP82-00357R000700120015-0